



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/829,763

04/10/2001

Osamu Shibata

29288.0400

9593

20322

7590

09/08/2005

SNELL & WILMER  
ONE ARIZONA CENTER  
400 EAST VAN BUREN  
PHOENIX, AZ 850040001

EXAMINER

PICH, PONNOREAY

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/829,763

Applicant(s)

SHIBATA ET AL.

Examiner

Ponnoreay Pich

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

Claims 1-4 were amended. Claims 5-9 were newly added. Claims 1-9 are pending.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action. The previous office action(s) is/are incorporated by reference in its/their entirety. The examiner assumes that the applicant agrees with any well-known prior art statements and/or rejections made by the examiner in the previous office action(s) that were not argued. Any objections or rejections not repeated below for record are withdrawn due to applicant's amendments and/or arguments.

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/27/2005 has been entered.

### ***Docketing***

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

### ***Response to Arguments***

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. In claim 3, it is unclear what "store the encrypted content key", the storage device or the mutual authentication section.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al (Us 5,923,754) in view of Venkatesan et al (US 6,801,999), herein referred to as Ven.

**Claim 1:**

Angelo discloses the limitations of:

1. An internal-key storage section operable to store an internal key (Fig 2, items 42 and 44; col 3, lines 50-58; and col 4, lines 31-33).

2. A content-key storage section operable to store content-keys (Fig 3, items 62 and 64; col 3, lines 50-58; and col 4, lines 41-67).
3. An operation section, the operating section including:
  - a. A first decryption section operable to, when an encrypted content-key is input to the operation section, decrypt the encrypted content-key using the internal-key so as to obtain a content-key and store the content-key in the content-key storage section (Fig 3, item 66; col 3, lines 58-62; and col 4, lines 59-61).
  - b. A second decrypting section operable to, when an encrypted content is input to the operation section, decrypt the encrypted content using the current value of the content-key storage section as a content-key so as to obtain a first output data and output the first output data to the outside of the decryption device (Fig 3, items 68-72; col 3, lines 58-62; and col 4, lines 61-67).

Angelo does not explicitly disclose a determination section operable to determine whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different.

However, Ven teaches determining a whether or not a watermark key has expired, the keys being such that they routinely expire after a given interval of time (col 7, lines 48-51). This teaching by Ven reads on the above limitation not met by Angelo. In light of Ven's teaching, it would have been obvious to one of ordinary skill in the art at

Art Unit: 2135

the time the applicant's invention was made to have modified Angelo's invention according to the limitations recited in claim 1. One of ordinary skill would have been motivated to do so as Ven discloses his teachings would reduce, if not, halt expanding security breach of protected objects when knowledge of compromised keys spread across a large user community (col 7, lines 54-59).

**Claim 2:**

Angelo and Ven disclose all the limitations recited in claim 1. Angelo further discloses the limitations of:

1. A content-key generation section operable to generate a content-key used for encrypting a content based on random numbers and store the generated content-key in the content-key storage section (col 4, lines 41-52), wherein the operation section further includes:
2. A first encryption section operable to encrypt the content-key used for encrypting a content so as to obtain an encrypted content-key and output the encrypted content-key to outside of the decryption device (col 3, lines 51-62 and col 4, lines 57-59).
3. A second encryption section operable to, when a content is input to the operation section, output the second output data to the outside of the decryption device (col 3, lines 51-62).

Further, the limitation of “the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different” is disclosed by Ven (col 7, lines 48-51).

**Claim 3:**

Angelo and Ven disclose all the limitations of claim 1. Angelo further discloses the limitations of:

1. A mutual authentication section operable to determine whether or not a mutual authentication has been made between the mutual authentication section and a storage device which is located outside the decryption device and store the encrypted content-key (col 4, lines 42-52).
2. Wherein the second decryption section is operable to decrypt the encrypted content when the mutual authentication section determines that the mutual authentication has been made (col 4, lines 57-67).

**Claim 4:**

Angelo and Ven disclose all the limitations of claim 1. Angelo further discloses the limitations of:

1. The internal storage section is operable to store a plurality of internal-keys (col 4, lines 31-33 and Fig 2).
2. The internal-key storage section is operable to select one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device (Fig 3).

**Claim 5:**

Angelo and Ven disclose all the limitations of claim 1. Further, Ven discloses the second decryption section is further operable to prevent decryption of the encrypted content when the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same (col 7, lines 48-51 and col 8, lines 46-51).

**Claim 6:**

Angelo discloses a method for decrypting encrypted content in a decryption device including an internal-key storage section and a content-key storage section, the method comprising:

1. Storing an internal-key in the internal-key storage section (Fig 2, items 42 and 44; col 3, lines 50-58; and col 4, lines 31-33).
2. Storing content-keys in the content-key storage section (Fig 3, items 62 and 64; col 3, lines 50-58; and col 4, lines 41-67).
3. Decrypting an encrypted content-key provided to the decryption device by using the internal-key so as to obtain a content key and storing the content-key in the content-key storage section (Fig 3, item 66; col 3, lines 58-62; and col 4, lines 59-61).
4. Decrypting the encrypted content using the current value of the content-key storage section as the content-key so as to obtain a first output data and output the first output data to outside of the decryption device (Fig 3, items 68-72; col 3, lines 58-62; and col 4, lines 61-67).

Angelo does not explicitly disclose the limitation of:

1. **When it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, decrypting the encrypted content.**

However, Ven teaches determining a whether or not a watermark key has expired, the keys being such that they routinely expire after a given interval of time (col 7, lines 48-51). This teaching by Ven reads on the above limitation not met by Angelo. In light of Ven's teaching, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Angelo's invention according to the limitations recited in claim 6. One of ordinary skill would have been motivated to do so as Ven discloses his teachings would reduce, if not, halt expanding security breach of protected objects when knowledge of compromised keys spread across a large user community (col 7, lines 54-59).

**Claim 7:**

Angelo and Ven disclose all the limitations of claim 6. Angelo further discloses the limitations of:

1. Generating a content-key used for encrypting a content based on random numbers and storing the generated content-key in the content key storage section (col 4, lines 41-52).

2. Encrypting the content-key used for encrypting the content so as to obtain an encrypted content-key and outputting the encrypted content-key to outside of the decryption device (col 3, lines 51-62 and col 4, lines 57-59).
3. Encrypting the content using the current value of the content-key storage section as a content-key so as to obtain a second output data and output the second output data to outside of the decryption device (col 3, lines 51-62).

Further, Ven discloses the limitation of “when it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different” (col 7, lines 48-51).

**Claim 8:**

Angelo and Ven disclose all the limitations of claim 6. Angelo further discloses the limitations of:

1. Storing a plurality of internal-keys in the internal-key storage section (col 4, lines 31-33 and Fig 2).
2. Selecting one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device (Fig 3).

**Claim 9:**

Angelo and Ven disclose all the limitations of claim 6. Ven further discloses the limitation of “preventing decryption of the encrypted content when it is determined that

the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same" (col 7, lines 48-51 and col 8, lines 46-51).


***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100